Cloud Compliance Center - Mexico

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

Mexico

*This content was last reviewed around July 2023.*

**Cloud friendly**

**1. Are financial institutions legally permitted to use cloud services?**

Yes. Financial institutions in Mexico (e.g., banks, financial technology institutions (such as e-wallet and crowdfunding entities) and brokerage firms) are permitted to contract with third-party service providers for the provision of cloud services. However, such arrangements are regarded and regulated as a form of "outsourcing." As a result, in some circumstances, financial institutions need to provide notice or obtain authorization from the National Banking and Securities Commission (CNBV) prior to contracting with third-party service providers for the provision of cloud services.

In general, the CNBV does not proactively encourage nor prevent private financial institutions from moving to the cloud. However, the fact that the CNBV expressly included a reference to crowdfunding and e-wallet institutions of "cloud services" contracting with third-party service providers in its General Rules Applicable to Financial Technology Institutions and General Rules Applicable to Electronic Payment Fund Institutions (which were published in 2018 and 2020 respectively) suggests that the CNBV is willing to acknowledge cloud services as a new standard.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes, outsourcing by financial institutions — including in respect of cloud services — is regulated, and some specific requirements apply in relation to providing cloud services to financial institutions.

The laws that regulate each kind of financial institution set out the requirements that such institutions must comply with to achieve authorization to procure sourced cloud services.

Article 328 of the General Rules Applicable to Banks (the "Circular Única de Bancos") sets out the rules regarding outsourcing by banks (institución de crédito)

Articles 44, 45, 50 and 51 of the General Rules Applicable to Electronic Payment Fund Institutions ("Disposiciones aplicables a las instituciones de fondos de pago electrónico a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera") set out the rules regarding outsourcing by e-wallet institutions (institución de fondos de pago electrónico)

Articles 85, 86 and 87 of the General Rules Applicable to Financial Technology Institutions ("Disposiciones de Caracter General Aplicables a las Instituciones de Tecnología Financiera") set out the rules regarding outsourcing by crowdfunding institutions (institución de financiamiento colectivo)

Article 206 of the General Rules Applicable to Brokerage (the "Circular Única de Casas de Bolsa") sets out the rules regarding outsourcing by brokerage firms (casa de bolsa)

In addition, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") applies to any financial institution that processes personal data. In that regard, the restrictions and requirements for private entities using cloud services to process personal data would apply.

**3. Are there any specific contractual requirements for cloud outsourcing?**

In general terms (as requirements can slightly vary depending on each financial institution), a financial institution that intends to engage a third-party service provider to provide cloud services to it on an outsourced basis must provide the National Banking and Securities Commission (CNBV) with a copy of the draft contract for the rendering of cloud services. The draft contract must indicate the probable date of its execution, and the rights and obligations of the financial institution and the third party. Additionally, the outsourcing contract must include a record of the third party's express acceptance of certain specific obligations, including obligations to do the following:

a) Deliver, during the course of an audit and at the financial institution's request, to the appointed independent external auditor and to the CNBV, the books, systems, records, manuals and documents in general that are related to the rendering of the service in question (The third party must also expressly accept an obligation to allow the independent external auditor or the CNBV's personnel access to its offices and facilities in general, related to the rendering of the service in question.)

b) Inform the financial institution of any modification to its corporate purpose or any other change that may affect the rendering of the service that is the object of the contract at least 30 days prior to such modification or change

c) Keep confidential the information that has been received, transmitted, processed or stored during the provision of the services and, likewise, accept that such information may only be used and exploited for the purposes agreed on in the provision of the service

Additionally, financial institutions are required to describe the following to the CNBV (among other requirements):

Type of cloud, whether public, private or hybrid

Specific regions where the information will be stored and processed

In public clouds or virtualization schemes on infrastructure shared with other clients, a description of the control mechanisms that will be used to guarantee the confidentiality, integrity and availability of sensitive information

In addition, in compliance with the requirements and restrictions contained in the implementing regulations of the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP), the agreement with the cloud service provider should confirm the following:

(i) The cloud service provider complies, at least, with the following: (a) have and apply personal data protection policies in accordance with the applicable principles and duties established in the LFPDPPP and related regulations; (b) be transparent in subcontracting involving the information in respect of which the service is provided; (c) refrain from including conditions for the provision of the service that authorize or allow it to assume ownership or ownership of the information in respect of which the service is provided, and (d) maintain confidentiality of the personal data in respect of which the service is provided.

(ii) The cloud service provider has mechanisms in place, at least, to: (a) make known changes in its privacy policies or conditions for the service it provides; (b) allow a data controller to limit the type of processing of the personal data in respect of which the service is provided; (c) establish and maintain adequate security measures for the protection of the personal data in respect of which the service is provided; (d) guarantee the deletion of the personal data once the service has been provided to the data controller and the data controller has been able to recover it; and (e) prevent access to the personal data to persons who do not have access privileges or, in the case of a founded and motivated request from a competent authority, inform the data controller of that fact.

**4. When does cloud outsourcing fall within the scope of the rules?**

In general terms, an arrangement will be regarded as cloud outsourcing within the scope of the rules when a financial institution (except for an e-wallet or crowdfunding institution) contracts with a third-party service provider for the rendering of operational processes or the administration of databases and computer systems (i.e., cloud services). Generally, 30 days' prior notice must be given to the National Banking and Securities Commission (CNBV) when such services are to be provided directly from Mexico by a local service provider. However, where a bank contracts for these services, advance authorization from the CNBV would be required where such services are provided or executed partially or entirely from abroad by a foreign service provider, without taking into account whether such services affect qualitatively or quantitatively the applicable financial institution's operation.

As for e-wallet and crowdfunding institutions, advance authorization from the CNBV and the Bank of Mexico will be required if an e-wallet/crowdfunding institution intends to contract with a third-party service provider that will carry out the transmission, storage, processing, safekeeping or custody of personal or sensitive information, personal identification documents issued by official authorities or biometric information of the e-wallet/crowdfunding institution's users, and only if the service provider (i.e., a cloud service provider) has privileged access to and control of said information or its security configuration. If the cloud service provider will not have access to nor control of the information held in the cloud, authorization from the CNBV is not required.

In addition, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP) applies where personal data is processed by a financial institution located in Mexico. The extraterritorial application of the LFPDPPP is limited but encompasses processing by a foreign entity (e.g., a cloud service provider) on behalf of a data controller based in Mexico. However, the particular requirements and restrictions to use cloud services for the processing of personal data are only triggered when the data controller adheres to the service provider's terms and conditions by means of general contracting conditions or clauses.

**5. Does the outsourcing need to be notified to the regulator?**

Sometimes. It is a requirement to obtain prior authorization from or give notice to the National Banking and Securities Commission (CNBV) before contracting with a third-party service provider for the provision of cloud services if the cloud services will be rendered totally or partially from abroad. For example, when contracting to receive cloud services provided totally or partially from offshore by third-party cloud service providers, banks must obtain authorization from the CNBV, while brokerage firms must only provide a prior 20 business days' notice to the CNBV. As described in the response to the question "Are there any specific contractual requirements for cloud outsourcing?", financial institutions are required to provide general information to the CNBV on the type of cloud services they are contracting to receive from a third-party service provider.

With respect to crowdfunding and e-wallet entities, prior authorization from the CNBV is required where a cloud service provider will act as a primary service provider and will have privileged access to sensitive information, biometric data and/or copies of official identification documents. However, where the cloud service provider will not have privileged access to such information/documents, authorization would not be required from the CNBV.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

If a financial institution does not comply with the regulatory requirements applicable to it, the National Banking and Securities Commission (CNBV) can request that the institution terminate the contractual relationship with the cloud service provider. It can also potentially impose administrative sanctions on the financial institution (these sanctions will be determined by the authority on a case-by-case basis and may vary depending on the severity of the breach).

In addition, from a privacy perspective, not complying with the requirements set forth by the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") could result in the imposition of a fine on the data controller. See the response to the question on data privacy and/or data security laws for more information.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes. General data privacy regulations — primarily, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP) — regulates how financial institutions handle the personal data of data subjects, such as employees, customers, users, suppliers, contractors and even cloud service providers.

Under the LFPDPPP, data controllers are restricted from contracting with cloud service providers that do not ensure proper protection of personal data, and they must not include terms or conditions in their contracts that would authorize or permit a cloud service provider to assume the ownership of personal data.

The LFPDPPP also requires a data controller to put in place a data processor agreement with an unrelated third party that will manage hosted personal data for the data controller. The data processor agreement must include certain terms, including provisions setting out the data processor's obligations and liabilities, restrictions relating to the data, and security measures to be taken.

Additionally, the Ministry of Economy and the data privacy authorities have issued a joint publication of the Minimum Suggested Criteria that Should be Considered for Contracting Cloud Computing Services that Involve Processing of Personal Data ("Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales," "**MSC Document**"). Given the collaborative nature of this document, not all the recommendations are specifically privacy-related. However, the MSC Document offers insight on the rationale and scope of the regulatory requirements. From the MSC Document, it can be inferred that a cloud service would be considered "secure" when data controllers do the following:

(a) Carry out certain pre-contractual screening of the cloud providers

(b) Ensure they are able to maintain control over their information placed in the cloud through contractual and technical mechanisms

(c) Ensure security measures are in place to protect the information

The MSC Document confirms that data controllers are liable for selecting and contracting the right cloud providers and that failure to carry out the minimum required tests appropriately would result in a breach of the Accountability Principle in the LFPDPPP and may be subject to fines.

Conversely, the MSC Document clarifies that cloud service providers are not legally mandated to include literally the requirements of Section 52 of the LFPDPPP in their contractual terms to convince customers that their services are compliant. Conversely, customers may use product literature, technical controls and other information that cloud service providers may offer to clients to evaluate the service as a whole and conclude whether their cloud offering is "secure." It is also clarified that cloud providers are subject to the general regime applicable to data processors, including, for instance, provisions related to subcontracting.

It is recommended to encrypt data hosted in a cloud service to protect the confidentiality of users' data. However, this is not a mandatory requirement under the applicable laws or regulations.

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

No. However, depending on the entity that manages the hosting, there may be particular requirements (e.g., if the hosting is carried out by a third party, it would be mandatory that the financial institution and the cloud service provider enter into an agreement, or if the hosting is conducted by an entity that is part of the same corporate group as the financial institution, having intragroup policies might be sufficient).

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No, cloud service providers do not require a license/authorization from the Mexican regulators to provide cloud services. However, depending on the specific type of financial institution, a prior authorization or notice from the National Banking and Securities Commission would be required; however, this obligation would only apply to the relevant financial institution and not directly to the cloud service provider.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

Express consent is not required where data is transferred to cloud service providers for the sole purpose of complying with a contract for providing financial services to the data subject.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

No, there is no Mexican law that requires a cloud service provider to be able to access the data it hosts.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes. Disclosing data to third parties is permitted when it is required by a competent authority through a judicial order or administrative request. Otherwise, there is no specific requirement in Mexican law that requires cloud service providers to disclose data hosted for financial institutions to financial authorities.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes. Financial institutions in Mexico (e.g., banks, financial technology institutions (such as e-wallet and crowdfunding entities) and brokerage firms) are permitted to contract with third-party service providers for the provision of cloud services. However, such arrangements are regarded and regulated as a form of "outsourcing." As a result, in some circumstances, financial institutions need to provide notice or obtain authorization from the National Banking and Securities Commission (CNBV) prior to contracting with third-party service providers for the provision of cloud services.

In general, the CNBV does not proactively encourage nor prevent private financial institutions from moving to the cloud. However, the fact that the CNBV expressly included a reference to crowdfunding and e-wallet institutions of "cloud services" contracting with third-party service providers in its General Rules Applicable to Financial Technology Institutions and General Rules Applicable to Electronic Payment Fund Institutions (which were published in 2018 and 2020 respectively) suggests that the CNBV is willing to acknowledge cloud services as a new standard.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes, outsourcing by financial institutions — including in respect of cloud services — is regulated, and some specific requirements apply in relation to providing cloud services to financial institutions.

The laws that regulate each kind of financial institution set out the requirements that such institutions must comply with to achieve authorization to procure sourced cloud services.

Article 328 of the General Rules Applicable to Banks (the "Circular Única de Bancos") sets out the rules regarding outsourcing by banks (institución de crédito)

Articles 44, 45, 50 and 51 of the General Rules Applicable to Electronic Payment Fund Institutions ("Disposiciones aplicables a las instituciones de fondos de pago electrónico a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera") set out the rules regarding outsourcing by e-wallet institutions (institución de fondos de pago electrónico)

Articles 85, 86 and 87 of the General Rules Applicable to Financial Technology Institutions ("Disposiciones de Caracter General Aplicables a las Instituciones de Tecnología Financiera") set out the rules regarding outsourcing by crowdfunding institutions (institución de financiamiento colectivo)

Article 206 of the General Rules Applicable to Brokerage (the "Circular Única de Casas de Bolsa") sets out the rules regarding outsourcing by brokerage firms (casa de bolsa)

In addition, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") applies to any financial institution that processes personal data. In that regard, the restrictions and requirements for private entities using cloud services to process personal data would apply.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

In general terms (as requirements can slightly vary depending on each financial institution), a financial institution that intends to engage a third-party service provider to provide cloud services to it on an outsourced basis must provide the National Banking and Securities Commission (CNBV) with a copy of the draft contract for the rendering of cloud services. The draft contract must indicate the probable date of its execution, and the rights and obligations of the financial institution and the third party. Additionally, the outsourcing contract must include a record of the third party's express acceptance of certain specific obligations, including obligations to do the following:

a) Deliver, during the course of an audit and at the financial institution's request, to the appointed independent external auditor and to the CNBV, the books, systems, records, manuals and documents in general that are related to the rendering of the service in question (The third party must also expressly accept an obligation to allow the independent external auditor or the CNBV's personnel access to its offices and facilities in general, related to the rendering of the service in question.)

b) Inform the financial institution of any modification to its corporate purpose or any other change that may affect the rendering of the service that is the object of the contract at least 30 days prior to such modification or change

c) Keep confidential the information that has been received, transmitted, processed or stored during the provision of the services and, likewise, accept that such information may only be used and exploited for the purposes agreed on in the provision of the service

Additionally, financial institutions are required to describe the following to the CNBV (among other requirements):

Type of cloud, whether public, private or hybrid

Specific regions where the information will be stored and processed

In public clouds or virtualization schemes on infrastructure shared with other clients, a description of the control mechanisms that will be used to guarantee the confidentiality, integrity and availability of sensitive information

In addition, in compliance with the requirements and restrictions contained in the implementing regulations of the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP), the agreement with the cloud service provider should confirm the following:

(i) The cloud service provider complies, at least, with the following: (a) have and apply personal data protection policies in accordance with the applicable principles and duties established in the LFPDPPP and related regulations; (b) be transparent in subcontracting involving the information in respect of which the service is provided; (c) refrain from including conditions for the provision of the service that authorize or allow it to assume ownership or ownership of the information in respect of which the service is provided, and (d) maintain confidentiality of the personal data in respect of which the service is provided.

(ii) The cloud service provider has mechanisms in place, at least, to: (a) make known changes in its privacy policies or conditions for the service it provides; (b) allow a data controller to limit the type of processing of the personal data in respect of which the service is provided; (c) establish and maintain adequate security measures for the protection of the personal data in respect of which the service is provided; (d) guarantee the deletion of the personal data once the service has been provided to the data controller and the data controller has been able to recover it; and (e) prevent access to the personal data to persons who do not have access privileges or, in the case of a founded and motivated request from a competent authority, inform the data controller of that fact.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

In general terms, an arrangement will be regarded as cloud outsourcing within the scope of the rules when a financial institution (except for an e-wallet or crowdfunding institution) contracts with a third-party service provider for the rendering of operational processes or the administration of databases and computer systems (i.e., cloud services). Generally, 30 days' prior notice must be given to the National Banking and Securities Commission (CNBV) when such services are to be provided directly from Mexico by a local service provider. However, where a bank contracts for these services, advance authorization from the CNBV would be required where such services are provided or executed partially or entirely from abroad by a foreign service provider, without taking into account whether such services affect qualitatively or quantitatively the applicable financial institution's operation.

As for e-wallet and crowdfunding institutions, advance authorization from the CNBV and the Bank of Mexico will be required if an e-wallet/crowdfunding institution intends to contract with a third-party service provider that will carry out the transmission, storage, processing, safekeeping or custody of personal or sensitive information, personal identification documents issued by official authorities or biometric information of the e-wallet/crowdfunding institution's users, and only if the service provider (i.e., a cloud service provider) has privileged access to and control of said information or its security configuration. If the cloud service provider will not have access to nor control of the information held in the cloud, authorization from the CNBV is not required.

In addition, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP) applies where personal data is processed by a financial institution located in Mexico. The extraterritorial application of the LFPDPPP is limited but encompasses processing by a foreign entity (e.g., a cloud service provider) on behalf of a data controller based in Mexico. However, the particular requirements and restrictions to use cloud services for the processing of personal data are only triggered when the data controller adheres to the service provider's terms and conditions by means of general contracting conditions or clauses.

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

Sometimes. It is a requirement to obtain prior authorization from or give notice to the National Banking and Securities Commission (CNBV) before contracting with a third-party service provider for the provision of cloud services if the cloud services will be rendered totally or partially from abroad. For example, when contracting to receive cloud services provided totally or partially from offshore by third-party cloud service providers, banks must obtain authorization from the CNBV, while brokerage firms must only provide a prior 20 business days' notice to the CNBV. As described in the response to the question "Are there any specific contractual requirements for cloud outsourcing?", financial institutions are required to provide general information to the CNBV on the type of cloud services they are contracting to receive from a third-party service provider.

With respect to crowdfunding and e-wallet entities, prior authorization from the CNBV is required where a cloud service provider will act as a primary service provider and will have privileged access to sensitive information, biometric data and/or copies of official identification documents. However, where the cloud service provider will not have privileged access to such information/documents, authorization would not be required from the CNBV.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

If a financial institution does not comply with the regulatory requirements applicable to it, the National Banking and Securities Commission (CNBV) can request that the institution terminate the contractual relationship with the cloud service provider. It can also potentially impose administrative sanctions on the financial institution (these sanctions will be determined by the authority on a case-by-case basis and may vary depending on the severity of the breach).

In addition, from a privacy perspective, not complying with the requirements set forth by the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") could result in the imposition of a fine on the data controller. See the response to the question on data privacy and/or data security laws for more information.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes. General data privacy regulations — primarily, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP) — regulates how financial institutions handle the personal data of data subjects, such as employees, customers, users, suppliers, contractors and even cloud service providers.

Under the LFPDPPP, data controllers are restricted from contracting with cloud service providers that do not ensure proper protection of personal data, and they must not include terms or conditions in their contracts that would authorize or permit a cloud service provider to assume the ownership of personal data.

The LFPDPPP also requires a data controller to put in place a data processor agreement with an unrelated third party that will manage hosted personal data for the data controller. The data processor agreement must include certain terms, including provisions setting out the data processor's obligations and liabilities, restrictions relating to the data, and security measures to be taken.

Additionally, the Ministry of Economy and the data privacy authorities have issued a joint publication of the Minimum Suggested Criteria that Should be Considered for Contracting Cloud Computing Services that Involve Processing of Personal Data ("Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales," "**MSC Document**"). Given the collaborative nature of this document, not all the recommendations are specifically privacy-related. However, the MSC Document offers insight on the rationale and scope of the regulatory requirements. From the MSC Document, it can be inferred that a cloud service would be considered "secure" when data controllers do the following:

(a) Carry out certain pre-contractual screening of the cloud providers

(b) Ensure they are able to maintain control over their information placed in the cloud through contractual and technical mechanisms

(c) Ensure security measures are in place to protect the information

The MSC Document confirms that data controllers are liable for selecting and contracting the right cloud providers and that failure to carry out the minimum required tests appropriately would result in a breach of the Accountability Principle in the LFPDPPP and may be subject to fines.

Conversely, the MSC Document clarifies that cloud service providers are not legally mandated to include literally the requirements of Section 52 of the LFPDPPP in their contractual terms to convince customers that their services are compliant. Conversely, customers may use product literature, technical controls and other information that cloud service providers may offer to clients to evaluate the service as a whole and conclude whether their cloud offering is "secure." It is also clarified that cloud providers are subject to the general regime applicable to data processors, including, for instance, provisions related to subcontracting.

It is recommended to encrypt data hosted in a cloud service to protect the confidentiality of users' data. However, this is not a mandatory requirement under the applicable laws or regulations.

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

No. However, depending on the entity that manages the hosting, there may be particular requirements (e.g., if the hosting is carried out by a third party, it would be mandatory that the financial institution and the cloud service provider enter into an agreement, or if the hosting is conducted by an entity that is part of the same corporate group as the financial institution, having intragroup policies might be sufficient).

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No, cloud service providers do not require a license/authorization from the Mexican regulators to provide cloud services. However, depending on the specific type of financial institution, a prior authorization or notice from the National Banking and Securities Commission would be required; however, this obligation would only apply to the relevant financial institution and not directly to the cloud service provider.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

Express consent is not required where data is transferred to cloud service providers for the sole purpose of complying with a contract for providing financial services to the data subject.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

No, there is no Mexican law that requires a cloud service provider to be able to access the data it hosts.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes. Disclosing data to third parties is permitted when it is required by a competent authority through a judicial order or administrative request. Otherwise, there is no specific requirement in Mexican law that requires cloud service providers to disclose data hosted for financial institutions to financial authorities.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.